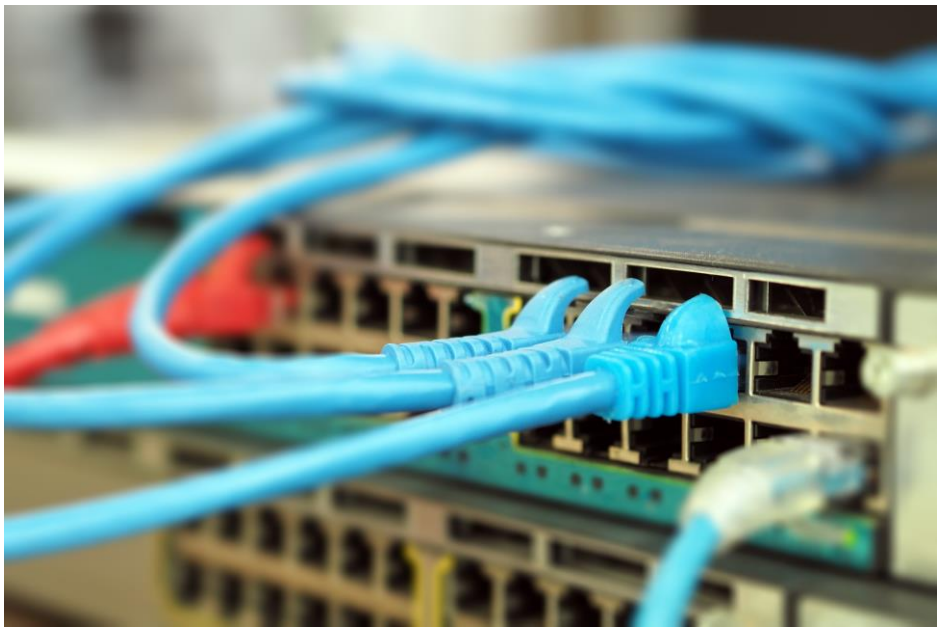

Understanding Networking Devices - A Brief Introduction
By TechLinu.com
Techlinu

Understanding Networking Devices – A Brief Introduction

All but the most basic of networks require devices to provide connectivity and functionality. Understanding how these networking devices operate and identifying the tasks they perform are important skills for any network administrator and requirements for a Network+ candidate.

This brief guide introduces usually used networking devices that you may encounter in your career as Network Administrator. This guide is also useful for BCS students and for passionate network learners.

Network HUBS



At the bottom of the networking food chain, so to speak, are hubs. Hubs are used in networks that use twisted-pair cabling to connect devices. Hubs can also be joined together to create larger networks. Hubs are simple devices that direct data packets to all devices connected to the hub, regardless of whether the data package is destined for the device. This makes them inefficient devices and can create a performance bottleneck on busy networks.

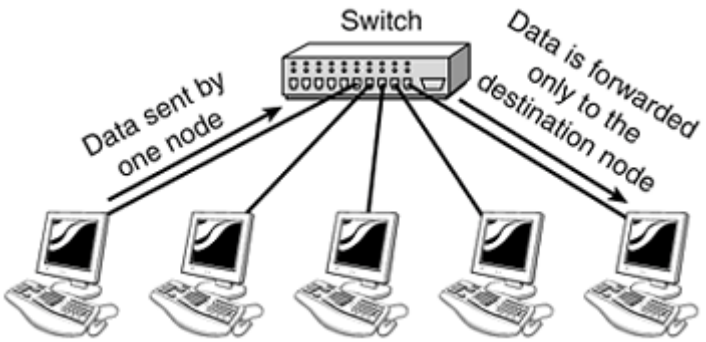
In its most basic form, a hub does nothing except provide a pathway for the electrical signals to travel along. Such a device is called a passive hub. Far more common nowadays is an active hub, which, as well as providing a path for the data signals, regenerates the signal before it forwards it to all of the connected devices. A hub does not perform any processing on the data that it forwards, nor does it perform any fault checking.

Hubs come in a variety of forms and sizes. Small hubs with five or eight connection ports are usually referred to as workgroup hubs. Others can accommodate larger numbers of devices (normally up to 32). These are referred to as high-density devices. Because hubs don't perform any processing, they do little except enable communication between connected devices. For today's high-demand network applications, something with a little more intelligence is required. That's where switches

come in.

Network Switches

Like hubs, switches are the connectivity points of an Ethernet network. Devices connect to switches via twisted-pair cabling, one cable for each device. The difference between hubs and switches is in how the devices deal with the data that they obtain. Whereas a hub forwards the data it receives to all of the ports on the device, a switch forwards it only to the port that connects to the destination device. It does this by learning the MAC address of the devices attached to it, and then by matching the destination MAC address in the data it receives. The **figure** below shows how a switch works.



By forwarding data only to the connection that should receive it, the switch can improve network performance in two ways. First, by creating a direct path between two devices and controlling their communication, it can really reduce the number of collisions on the network. As you might know, collisions occur on Ethernet networks when two devices attempt to transmit at exactly the same time. In addition, the lack of collisions enables switches to communicate with devices in full-duplex mode. In a full-duplex configuration, devices can send and receive data from the switch at the same time. Contrast this with half-duplex communication, in which communication can occur in only one direction at a time. Full-duplex transmissions speeds are double that of a standard, half-duplex, connection. So, a 10Mbps connection becomes 20Mbps, and a 100Mbps connection becomes 200Mbps.

The net result of these measures is that switches can offer significant performance improvements

over hub-based networks, particularly when network use is high.

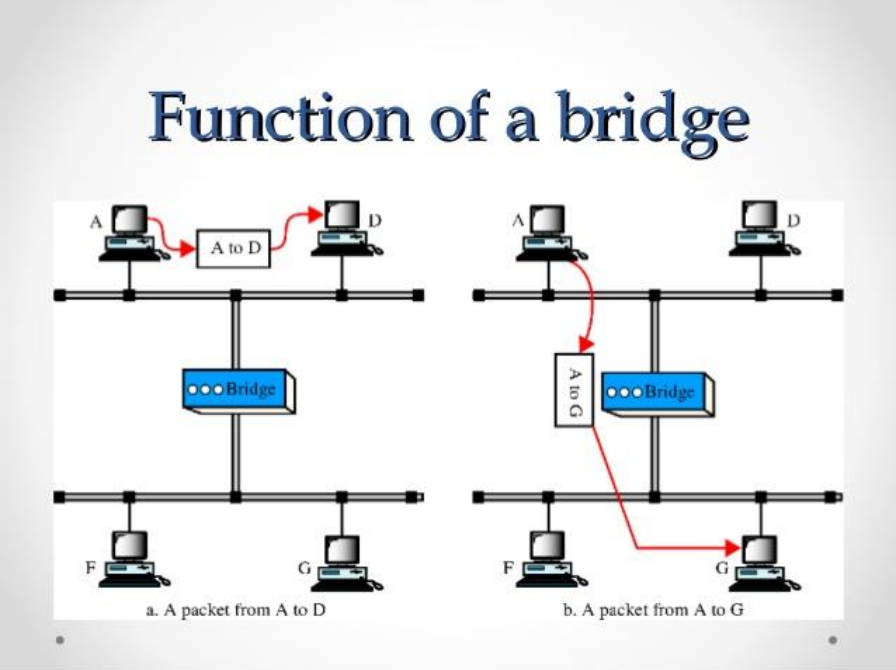
Irrespective of whether a connection is at full or half duplex, the technique of switching dictates how the switch deals with the data it receives. The following is a brief clarification of each method:

1. **Cut-through** — In a cut-through switching environment, the packet begins to be forwarded as soon as it is received. This method is very rapid, but creates the possibility of errors being propagated through the network, as there is no error checking.
2. **Store-and-forward** — Unlike cut-through, in a store-and-forward switching environment, the entire packet is received and error checked before being forwarded. The upside of this method is that errors are not propagated through the network. The downside is that the error checking process takes a relatively long time, and store-and-forward switching is considerably slower as a result.
3. **FragmentFree** — To take advantage of the error checking of store-and-forward switching, but still offer performance levels nearing that of cut-through switching, FragmentFree switching can be used. In a FragmentFree-switching environment, enough of the packet is read so that the switch can define whether the packet has been involved in a collision. As soon as the collision status has been defined, the packet is forwarded.

Network Bridges

Bridges are used to divide larger networks into smaller sections. They do this by sitting between two physical network segments and managing the flow of data between the two. By looking at the MAC address of the devices connected to each segment, bridges can elect to forward the data (if they believe that the destination address is on another interface), or block it from crossing (if they can verify that it is on the interface from which it came).

The **Figure** below shows how a bridge functions.



Note: Bridges can also be used to connect two physical LANs into a larger logical LAN.

When bridges were introduced, the MAC addresses of the devices on the connected networks had to be entered manually, a time-consuming process that had plenty of opportunity for error. Today, almost all bridges can build a list of the MAC addresses on an interface by watching the traffic on the network. Such devices are called learning bridges because of this functionality.

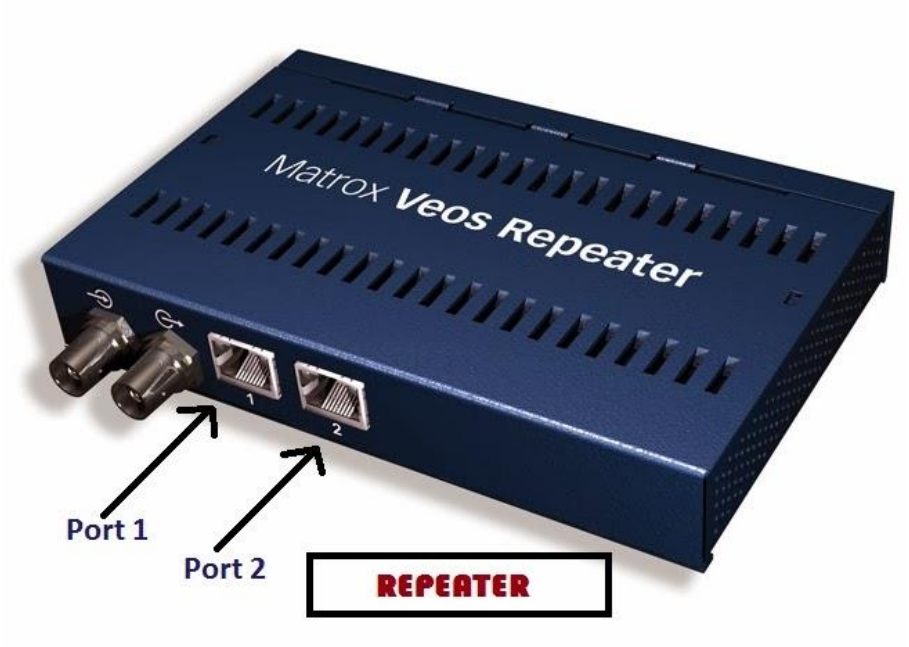
Kinds of Bridges

Three types of bridges are used in networks:

1. **Transparent bridge** — Derives its name from the fact that the devices on the network are unaware of its existence. A transparent bridge does nothing except block or forward data based on the MAC address.
2. **Source route bridge** — Used in Token Ring networks. The source route bridge derives its name from the fact that the entire path that the packet is to take through the network is embedded within the packet.
3. **Translational bridge** — Used to convert one networking data format to another; for example, from Token Ring to Ethernet and vice versa.

Today, bridges are slowly but surely falling out of favor. Ethernet switches offer similar functionality; they can provide logical divisions, or segments, in the network. In fact, switches are sometimes referred to as multiport bridges because of the way they operate.

Repeater



A repeater is an electronic device that amplifies the signal it receives. In other terms, you can think of repeater as a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances.

For example, inside a college campus, the hostels might be far away from the main college where the ISP line comes in. If the college authority wants to pull a wire in between the hostels and main campus, they will have to use repeaters if the distance is much because different types of cables have limitations in terms of the distances they can carry the data for.

When these network devices take a particular configurational shape on a network, their configuration gets a particular name and the whole formation is called Network topology. In certain circumstances when we add some more network devices to a network topology, it's called Daisy chaining.

Network Routers

In a common configuration, routers are used to create larger networks by joining two network segments. Such as a SOHO router used to connect a user to the Internet. A router can be a dedicated hardware device or a computer system with more than one network interface and the right routing software. All modern network operating systems include the functionality to act as a router.

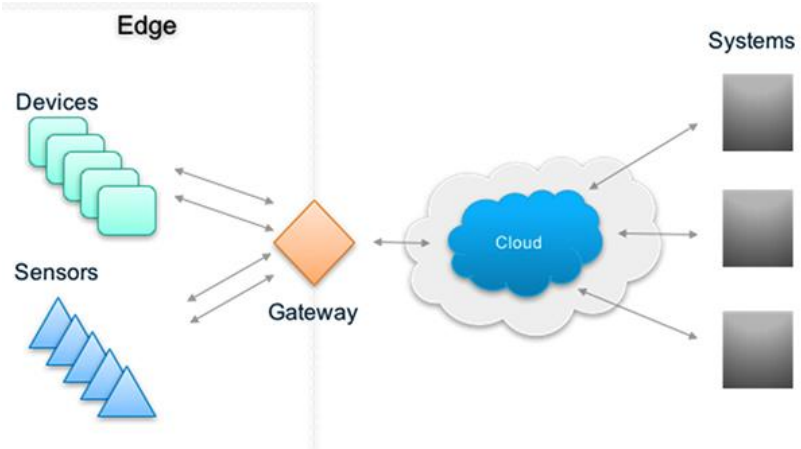
Routers will normally create, add, or divide on the Network Layer as they are normally IP-based devices.

A router derives its name from the fact that it can route data it receives from one network onto another. When a router receives a packet of data, it reads the header of the packet to define the destination address. Once it has defined the address, it looks in its routing table to determine whether it knows how to reach the destination and, if it does, it forwards the packet to the next hop on the route. The next hop might be the final destination, or it might be another router. The **Figure** below shows, in basic terms, how a router works.

A router determines how information is passed in the most efficient manner.

As you can see from this example, routing tables play a very important role in the routing process. They are the means by which the router makes its decisions. For this reason, a routing table needs to be two things. It must be up-to-date, and it must be complete. There are two ways that the router can get the information for the routing table—through static routing or dynamic routing.

Network Gateways



Any device that translates one data format to another is called a gateway. Some examples of gateways include a router that translates data from one network protocol to another, a bridge that converts between two networking systems, and a software application that converts between two different formats. The key point about a gateway is that only the data format is translated, not the data itself. In many cases, the gateway functionality is incorporated into another device.

CSU/DSU

A Channel Service Unit/Digital Service Unit (CSU/DSU), sometimes called Data Service Unit, is a device that converts the digital signal format used on LANs into one used on WANs. Such translation is necessary because the networking technologies used on WANs are different from those used on LANs.

The CSU/DSU sits between the LAN and the access point provided by the telecommunications company. Many router manufacturers are now incorporating CSU/DSU functionality into their products.

Network Cards (NICs)

Network cards, also called Network Interface Cards, are devices that enable computers to connect to the network.

When specifying or installing a NIC, you must consider the following issues:

1. **System bus compatibility** — If the network interface you are installing is an internal device, bus compatibility must be verified. The most common bus system in use is the Peripheral Component Interconnect (PCI) bus, but some older systems might still use Industry Standard Architecture (ISA) expansion cards.
2. **System resources** — Network cards, like other devices, need IRQ and memory I/O addresses. If the network card does not operate correctly after installation, there might be a device conflict.
3. **Media compatibility** — Today, the assumption is that networks use twisted-pair cabling, so if you need a card for coaxial or fiber-optic connections, you must specify this. Wireless network cards are also available.

Even more than the assumption you are using twisted-pair cabling is that the networking system being used is Ethernet. If you require a card for another networking system such as Token Ring, this must be specified when you order.

Note: When working on a Token Ring network, you have to ensure that all network cards are set to transmit at the same speeds. NICs on an Ethernet network can operate at various speeds.

To install or configure a network interface, you will need drivers of the device, and might need to configure it, although many devices are now plug and play. Most network cards are now software configured. Many of these software configuration utilities also include testing capabilities. The drivers and software configuration utilities supplied with the cards are often not the latest available, so it is best practice to log on to the Internet and download the latest drivers and associated software.

ISDN Adapters

Integrated Services Digital Network (ISDN) is a remote access and WAN technology that can be used

in place of a Plain Old Telephone Service (POTS) dial-up link if it is available. The availability of ISDN depends on whether your local telecommunications service provider offers the service, the quality of the line to your premises, and your proximity to the provider's location. ISDN offers greater speeds than a modem and can also pick up and drop the line considerably faster.

If ISDN is available and you do elect to use it, a special device called an ISDN terminal adapter is needed to connect to the line. ISDN terminal adapters can be add-in expansion cards, external devices that connect to the serial port of the system, or specialized interfaces built in to routers or other networking equipment. The ISDN terminal adapter is necessary because, although it uses digital signals, the signals are formatted differently from those used on a LAN. In addition, ISDN can create multiple communication channels on a single line. Today, ISDN is not widely deployed and has been replaced by faster and often cheaper technologies.

Wireless Access Points (APs)

Wireless access points (APs) are a transmitter and receiver (transceiver) device used to create a wireless LAN (WLAN). APs are typically a separate network device with a built-in antenna, transmitter, and adapter. APs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired Ethernet LAN. APs also typically have several ports allowing a way to expand the network to support additional clients.

Depending on the size of the network, one or more APs might be required. Additional APs are used to allow access to more wireless clients and to expand the range of the wireless network. Each AP is limited by a transmissions range—the distance a client can be from a AP and still get a useable signal. The actual distance depends on the wireless standard being used and the obstructions and environmental conditions between the client and the AP.

A **WAP** can operate as a bridge connecting a standard wired network to wireless devices or as a

router passing data transmissions from one access point to another.

Saying that an AP is used to extend a wired LAN to wireless clients doesn't give you the complete picture. A wireless AP today can provide different services in addition to just an access point. Today, the APs might provide many ports that can be used to easily increase the size of the network. Systems can be added and removed from the network with no effect on other systems on the network. Also, many APs provide firewall capabilities and DHCP service. When they are hooked up, they will provide client systems with a private IP address and then prevent Internet traffic from accessing client systems. So in effect, the AP is a switch, a DHCP Server, router, and a firewall.

APs come in all different shapes and sizes. Many are cheaper and designed strictly for home or small office use. Such APs have low powered antennas and limited expansion ports. Higher end APs used for commercial purposes have very high powered antennas enabling them to extend the range that the wireless signal can travel.

APs are used to create a wireless LAN and to extend a wired network. APs are used in the infrastructure wireless topology.

Modems

A modem, short for modulator/demodulator, is a device that converts the digital signals generated by a computer into analog signals that can travel over conventional phone lines. The modem at the receiving end converts the signal back into a format the computer can understand. Modems can be used as a means to connect to an ISP or as a mechanism for dialing up to a LAN.

Modems can be internal add-in expansion cards, external devices that connect to the serial or USB port of a system, PCMCIA cards designed for use in laptops, or proprietary devices designed for use on other devices such as portables and handhelds.

The configuration of a modem depends on whether it is an internal or external device. For internal devices, the modem must be configured with an interrupt request (IRQ) and a memory I/O address. It is common practice, when installing an internal modem, to disable the built-in serial interfaces and assign the modem the resources of one of those (typically COM2).

Transceivers (Media Converters)

The term transceiver does describe a separate network device, but it can also be technology built and embedded in devices such as network cards and modems. In a network environment, a transceiver gets its name from being both a transmitter and a receiver of signals—thus the name transceivers.

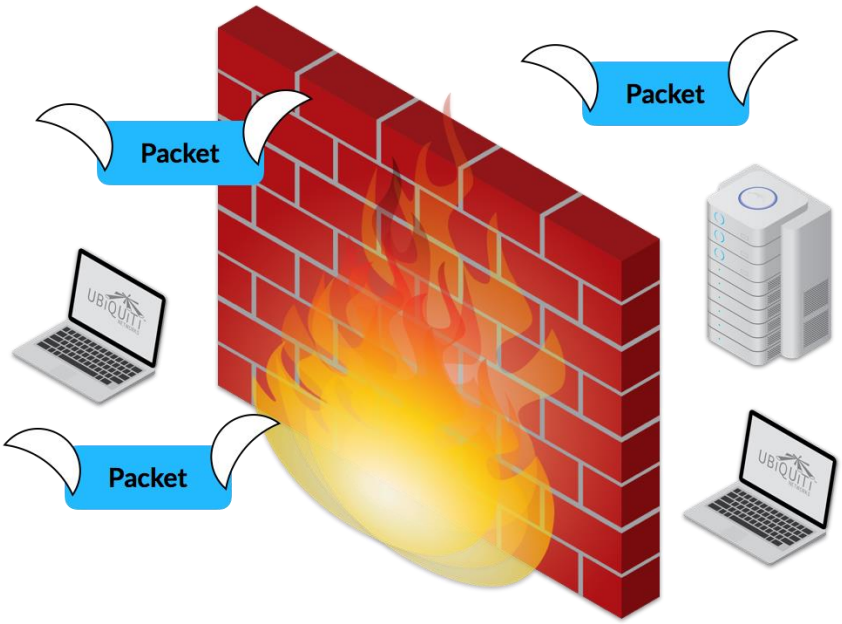
Technically, on a LAN, the transceiver is responsible for placing signals onto the network media and also detecting incoming signals traveling through the same wire. Given the description of the function of a transceiver, it makes sense that that technology would be found with network cards.

Although transceivers are found in network cards, they can be external devices as well. As far as networking is concerned, transceivers can ship as a module or chip type. Chip transceivers are small and are inserted into a system board or wired directly on a circuit board. Module transceivers are external to the network and are installed and function similarly to other computer peripherals, or they can function as standalone devices.

There are many types of transceivers—RF transceivers, fiber optic transceivers, Ethernet transceivers, wireless (WAP) transceivers, and more. Though each of these media types are different, the function of the transceiver remains the same. Each type of the transceiver used has different characteristics, such as the number of ports available to connect to the network and whether full-duplex communication is supported.

Listed with transceivers in the CompTIA objectives are media converters. Media converters are a technology that allows administrators to interconnect different media types—for example, twisted pair, fiber, and Thin or thick coax—within an existing network. Using a media converter, it is possible to connect newer 100Mbps, Gigabit Ethernet, or ATM equipment to existing networks such as 10BASE-T or 100BASE-T. They can also be used in pairs to insert a fiber segment into copper networks to increase cabling distances and enhance immunity to electromagnetic interference (EMI).

Firewalls



A firewall is a networking device, either hardware or software based, that controls access to your organization's network. This controlled access is designed to protect data and resources from an outside threat. To do this, firewalls are typically placed at entry/exit points of a network—for example, placing a firewall between an internal network and the Internet. Once there, it can control access in and out of that point.

Although firewalls typically protect internal networks from public networks, they are also used to control access between specific network segments within a network—for example, placing a firewall between the Accounts and the Sales departments.

As mentioned, firewalls can be implemented through software or through a dedicated hardware device. Organizations implement software firewalls through network operating systems (NOS) such as Linux/UNIX, Windows servers, and Mac OS servers. The firewall is configured on the server to allow or permit certain types of network traffic. In small offices and for regular home use, a firewall is commonly installed on the local system and configured to control traffic. Many third-party firewalls are available.

Hardware firewalls are used in networks of all sizes today. Hardware firewalls are often dedicated network devices that can be implemented with very little configuration and protect all systems behind the firewall from outside sources. Hardware firewalls are readily available and often combined with other devices today. For example, many broadband routers and wireless access points have firewall functionality built in. In such case, the router or WAP might have a number of ports available to plug systems in to.

Conclusion

Different networking devices have different roles to play in a computer network. These network devices also work at different segments of a computer network performing different works.